Claims:

1. A secure communication system comprising: a communications network; at a sending location on said network: (i) an encapsulator (1) for providing (a) a session key (K), and (b) a plurality of asymmetric encryptions of the session key (E1(K), E2(K), E3(K) ... Ei(K) ... En(K)), each said encryption corresponding to a respective receiving location (1 to n) on said network; and (ii) a symmetric encryptor (3) for utilising said session key (K) to encrypt a message (M); and, at each said receiving location (1 to n) on said network: (i) a decapsulator (5) for decrypting the encryption of said plurality of encryptions (E1(K), E2(K), E3(K) ... Ei(K) ... En(K)) which corresponds to that receiving location (1 to n) to provide said session key (K); and (ii) a symmetric decryptor (7) for utilising the session key (K) to decrypt the message (M), said encapsulator (1) comprising: a pseudo random number generator (51 or 91); symmetric key derivation means (55 or 95) for deriving said session key (K) from a first random number (N) generated by said pseudo random number generator (51 or 91); means (53 or 93) for utilising said first random number (N) to generate a second random number (r); and means (57-0 to 57-n and 59-1 to 59-n, or 97-1 to 97-n and 99-1 to 99-(n-1) and 101-(-1) to 101-(n-1) and 103 and 105 and 107) for utilising the first keys (pk1 to pkn, or id1 to idn) of asymmetric encryption key pairs (pk1 to pkn and sk1 to skn, or id1 to idn and S1 to Sn) of the intended recipients at the receiving locations (1 to n) together with said second random number (r) and said first random number (N) to generate said plurality of asymmetric encryptions of the session key (E1(K), E2(K), E3(K) ... Ei(K) ... En(K)), said decapsulator (5) at each receiving location (1 to n) comprising: means (71, 73, 75, or 111, 113, 115 or 131, 133, 135, 137, 139, 141) for utilising the second key (ski or Si) of the asymmetric encryption key pair (pki and ski, or idi and Si) of the

recipient at the receiving location together with the asymmetric encryption (Ei(K)) corresponding to the receiving location to recover said first random number (N); and a further symmetric key derivation means (77, or 117 or 143) for deriving said session key (K) from said first random number (N).

2. A secure communication system comprising: a communications network; at a sending location on said network an encryptor (1) for providing a plurality of asymmetric encryptions of a message (M), each said encryption corresponding to a respective receiving location (1 to n) on said network, said encryptor comprising: means (53 or 93) for deriving from said message (M) a first random number (r); and means (57-0 to 57-n and 59-1 to 59-n, or 97-1 to 97-n and 99-1 to 99-(n-1) and 101-(-1) to 101-(n-1) and 103 and 105 and 107) for utilising the first keys (pk1 to pkn, or id1 to idn) of asymmetric encryption key pairs (pk1 to pkn and sk1 to skn, or id1 to idn and S1 to Sn) of the intended recipients at the receiving locations (1 to n) together with said first random number (r) and said message (M) to generate said plurality of asymmetric encryptions of the message; and, at each said receiving location (1 to n) on said network a decryptor (5) for decrypting the encryption of said plurality of encryptions which corresponds to that receiving location (1 to n) to provide said message (M), said decryptor (5) comprising means (71, 73, 75, or 111, 113, 115 or 131, 133, 135, 137, 139, 141) for utilising the second key (ski or Si) of the asymmetric encryption key pair (pki and ski, or idi and Si) of the recipient at the receiving location together with the asymmetric encryption corresponding to the receiving location to recover the message (M).

3. A system according to claim 2 wherein: said first and second keys (pk1 to pkn, sk1 to skn) comprise public and private keys (pk1 to pkn, sk1 to skn) assigned to the

recipients as part of a public key cryptography communication scheme; said means (57-0 to 57-n, 59-1 to 59-n) for utilising the public keys (pk1 to pkn) comprises: a series of first exponentiation means (57-0 to 57-n), one of said first exponentiation means (57-0) raising a fixed system parameter (g) to the power of said first random number (r) to provide a first output (d), each of the remainder of said first exponentiation means (57-1 to 57-n) raising a respective public key (pk1 to pkn) to the power of said first random number (r) to provide a second output (pki^r); and a series of first multiplication means (59-1 to 59-n), each first multiplication means (59-1 to 59-n) multiplying a respective said second output (pki^r) by said message (M) to provide a third output (ci), said third outputs (ci) of said first multiplication means (59-1 to 59-n) together with said first output (d) of said one of said first exponentiation means (57-0) constituting said plurality of asymmetric encryptions of the message (M); and said means (71, 73, 75) for utilising the private key (ski) comprises: second exponentiation means (71) for raising said first output (d) to the power of the private key (ski); inversion means (73) for inverting the output (d^ski) of said second exponentiation means (71); and a second multiplication means (75) for multiplying the output (1/(d^ski)) of said inversion means (73) by the said third output (ci) corresponding to the receiving location (1 to n), said second multiplication means (75) thereby recovering the message (M).

4. A system according to claim 2 wherein: said first keys (id1 to idn) comprise identity keys (id1 to idn) based on the identities of the recipients, and said second keys (S1 to Sn) comprise corresponding secret keys (S1 to Sn) assigned to the recipients as part of an identity based cryptography communication scheme; said means (97-1 to 97-n, 99-1 to 99-(n-1), 101-(-1) to 101-(n-1), 103, 105, 107) for utilising the identity keys (id1 to idn) comprises: a series of first hash-to-point means (97-1 to 97-n), one of said

first hash-to-point means (97-1) utilising one of the identity keys (id1) to implement a first hash-to-point algorithm (H1) to provide a first output (Qid1), each remaining said first hash-to-point means (97-2 to 97-n) utilising a respective remaining identity key (id2 to idn) to implement said first hash-to-point algorithm (H1) to provide a second output (Qid2 to Qidn); a series of subtraction means (99-1 to 99-(n-1)), each said subtraction means (99-1 to 99-(n-1)) utilising said first output (Qid1) together with a respective said second output (Qid2 to Qidn) to implement a subtraction algorithm (SUB) to provide a third output (T1 to Tn); a series of first multiplication means (101-(-1) to 101-(n-1)), one of said first multiplication means (101-(-1)) utilising said first random number (r) and a fixed system parameter (P) to implement a multiplication algorithm (MULT) to provide a fourth output (U), another of said first multiplication means (101-0) utilising said first random number (r) and said first output (Qid1) to implement said multiplication algorithm (MULT) to provide a fifth output (U0), each remaining said first multiplication means (101-1 to 101-(n-1)) utilising said first random number (r) together with a respective said third output (T1 to Tn) to implement said multiplication algorithm (MULT) to provide a sixth output (U1 to U(n-1)); first pairing means (103) for utilising a publicly available key (R) together with said fifth output (U0) to implement a pairing algorithm (PAIR) to provide a seventh output (t); second hash-to-point means (105) for utilising said seventh output (t) to implement a second hash-to-point algorithm (H2) to provide an eighth output (W); and symmetric encryption means (107) for utilising said message (M) together with said eighth output (W) to implement a symmetric encryption function to provide a ninth output (V), said fourth, sixth and ninth outputs (U, U1 to U(n-1), V) together constituting said plurality of asymmetric encryptions of the message (M); and said means (111, 113, 115 or 131,

133, 135, 137, 139, 141) for utilising the secret key (Si) comprises: at one receiving location (1) of said receiving locations (1 to n): second pairing means (111) for utilising the secret key (S1) of the recipient at the receiving location (1) together with said fourth output (U) to implement said pairing algorithm (PAIR) to provide a tenth output (t); third hash-to-point means (113) for utilising said tenth output (t) to implement said second hash-to-point algorithm (H2) to provide an eleventh output (W); and symmetric decryption means (115) for utilising said eleventh output (W) together with said ninth output (V) to implement a symmetric decryption function corresponding to said symmetric encryption function to recover said message (M); and at each remaining receiving location (2 to n): third pairing means (131) for utilising the secret key (Si ($1 < i \leq n$)) of the recipient at the receiving location (2 to n) together with said fourth output (U) to implement said pairing algorithm (PAIR) to provide a twelfth output (t1); point negation means (135) for utilising the said sixth output (U1 to U(n-1)) corresponding to the receiving location (2 to n) to implement a point negation algorithm to provide a thirteenth output; fourth pairing means (137) for utilising said thirteenth output together with said publicly available key (R) to implement said pairing algorithm (PAIR) to provide a fourteenth output (t2); second multiplication means (133) for utilising said twelfth and fourteenth outputs (t1, t2) to implement said multiplication algorithm (MULT) to provide a fifteenth output (t); fourth hash-to-point means (139) for utilising said fifteenth output (t) to implement said second hash-to-point algorithm (H2) to provide a sixteenth output (W); and further symmetric decryption means (141) for utilising said sixteenth output (W) together with said ninth output (V) to implement a symmetric decryption function corresponding to said symmetric encryption function to recover said message (M).

5. A secure communication method comprising: at a sending location on a communications network: (i) providing (a) a session key (K), and (b) a plurality of asymmetric encryptions of the session key (E1(K), E2(K), E3(K) ... Ei(K) ... En(K)), each said encryption corresponding to a respective receiving location (1 to n) on said network; and (ii) utilising said session key (K) to encrypt symmetrically a message (M); and, at each said receiving location (1 to n) on said network: (i) decrypting the encryption of said plurality of encryptions (E1(K), E2(K), E3(K) ... Ei(K) ... En(K)) which corresponds to that receiving location (1 to n) to provide said session key (K); and (ii) utilising the session key (K) to decrypt the message (M), said step (i) carried out at the sending location comprising: generating a first random number (N); deriving said session key (K) from said first random number (N); utilising said first random number (N) to generate a second random number (r); and utilising the first keys (pk1 to pkn, or id1 to idn) of asymmetric encryption key pairs (pk1 to pkn and sk1 to skn, or id1 to idn and S1 to Sn) of the intended recipients at the receiving locations (1 to n) together with said second random number (r) and said first random number (N) to generate said plurality of asymmetric encryptions of the session key (E1(K), E2(K), E3(K) ... Ei(K) ... En(K)), said step (i) carried out at each receiving location (1 to n) comprising: utilising the second key (ski or Si) of the asymmetric encryption key pair (pki and ski, or idi and Si) of the recipient at the receiving location together with the asymmetric encryption (Ei(K)) corresponding to the receiving location to recover said first random number (N); and deriving said session key (K) from said first random number (N).

6. A secure communication method comprising: at a sending location on a communications network providing a plurality of asymmetric encryptions of a message (M), each said encryption corresponding to a respective receiving location (1 to n) on

said network, said step of providing said plurality of asymmetric encryptions comprising: deriving from said message (M) a first random number (r); and utilising the first keys (pk1 to pkn, or id1 to idn) of asymmetric encryption key pairs (pk1 to pkn and sk1 to skn, or id1 to idn and S1 to Sn) of the intended recipients at the receiving locations (1 to n) together with said first random number (r) and said message (M) to generate said plurality of asymmetric encryptions of the message; and, at each said receiving location (1 to n) on said network decrypting the encryption of said plurality of encryptions which corresponds to that receiving location (1 to n) to provide said message (M), said step of decrypting comprising utilising the second key (ski or Si) of the asymmetric encryption key pair (pki and ski, or idi and Si) of the recipient at the receiving location together with the asymmetric encryption corresponding to the receiving location to recover the message (M).

7. A method according to claim 6 wherein: said first and second keys (pk1 to pkn, sk1 to skn) comprise public and private keys (pk1 to pkn, sk1 to skn) assigned to the recipients as part of a public key cryptography communication scheme; said step of utilising the public keys (pk1 to pkn) comprises: raising a fixed system parameter (g) to the power of said first random number (r) to provide a first output (d); raising each public key (pk1 to pkn) to the power of said first random number (r) to provide a second output (pki^r); and multiplying each said second output (pki^r) by said message (M) to provide a third output (ci), said third outputs (ci) together with said first output (d) constituting said plurality of asymmetric encryptions of the message (M); and said step of utilising the private key (ski) comprises: raising said first output (d) to the power of the private key (ski) to provide a fourth output (d^ski); inverting the fourth output (d^ski) to provide a fifth output (1/(d^ski)); and multiplying the fifth output (1/(d^ski))

by the said third output (ci) corresponding to the receiving location (1 to n) to recover the message (M).

8. A method according to claim 6 wherein: said first keys (id1 to idn) comprise identity keys (id1 to idn) based on the identities of the recipients, and said second keys (S1 to Sn) comprise corresponding secret keys (S1 to Sn) assigned to the recipients as part of an identity based cryptography communication scheme; said step of utilising the identity keys (id1 to idn) comprises: utilising one of the identity keys (id1) to implement a first hash-to-point algorithm (H1) to provide a first output (Qid1); utilising each remaining identity key (id2 to idn) to implement said first hash-to-point algorithm (H1) to provide a second output (Qid2 to Qidn); utilising said first output (Qid1) together with each said second output (Qid2 to Qidn) to implement a subtraction algorithm (SUB) to provide a third output (T1 to Tn); utilising said first random number (r) and a fixed system parameter (P) to implement a multiplication algorithm (MULT) to provide a fourth output (U); utilising said first random number (r) and said first output (Qid1) to implement said multiplication algorithm (MULT) to provide a fifth output (U0); utilising said first random number (r) together with each said third output (T1 to Tn) to implement said multiplication algorithm (MULT) to provide a sixth output (U1 to U(n-1)); utilising a publicly available key (R) together with said fifth output (U0) to implement a pairing algorithm (PAIR) to provide a seventh output (t); utilising said seventh output (t) to implement a second hash-to-point algorithm (H2) to provide an eighth output (W); and utilising said message (M) together with said eighth output (W) to implement a symmetric encryption function to provide a ninth output (V), said fourth, sixth and ninth outputs (U, U1 to U(n-1), V) together constituting said plurality of asymmetric encryptions of the message (M); and said step of utilising the secret key

(Si) comprises: at one receiving location (1) of said receiving locations (1 to n): utilising the secret key (S1) of the recipient at the receiving location (1) together with said fourth output (U) to implement said pairing algorithm (PAIR) to provide a tenth output (t); utilising said tenth output (t) to implement said second hash-to-point algorithm (H2) to provide an eleventh output (W); and utilising said eleventh output (W) together with said ninth output (V) to implement a symmetric decryption function corresponding to said symmetric encryption function to recover said message (M); and at each remaining receiving location (2 to n): utilising the secret key (Si ($1 < i \leq n$)) of the recipient at the receiving location (2 to n) together with said fourth output (U) to implement said pairing algorithm (PAIR) to provide a twelfth output (t1); utilising the said sixth output (U1 to U(n-1)) corresponding to the receiving location (2 to n) to implement a point negation algorithm to provide a thirteenth output; utilising said thirteenth output together with said publicly available key (R) to implement said pairing algorithm (PAIR) to provide a fourteenth output (t2); utilising said twelfth and fourteenth outputs (t1, t2) to implement said multiplication algorithm (MULT) to provide a fifteenth output (t); utilising said fifteenth output (t) to implement said second hash-to-point algorithm (H2) to provide a sixteenth output (W); and utilising said sixteenth output (W) together with said ninth output (V) to implement a symmetric decryption function corresponding to said symmetric encryption function to recover said message (M).